

Private Broadcasting: an Index Coding Approach

Mohammed Karmoose, Linqi Song, Martina Cardone, Christina Fragouli

University of California Los Angeles, Los Angeles, CA 90095 USA

Email: {mkarmoose, songlinqi, martina.cardone, christina.fragouli}@ucla.edu

Abstract

Using a broadcast channel to transmit clients' data requests may impose privacy risks. In this paper, we address such privacy concerns in the index coding framework. We show how a malicious client can infer some information about the requests and side information of other clients by learning the encoding matrix used by the server. We propose an information-theoretic metric to measure the level of privacy and show how encoding matrices can be designed to achieve specific privacy guarantees. We then consider a special scenario for which we design a transmission scheme and derive the achieved levels of privacy in closed-form. We also derive upper bounds and we compare them to the levels of privacy achieved by our scheme, highlighting that an inherent trade-off exists between protecting privacy of the request and of the side information of the clients.

I. INTRODUCTION

Consider a set of clients who share the same broadcast domain and wish to download data content from a server. Even though the content that they request may be publicly available, they wish to preserve the anonymity of their requests. For instance, assume that a client requests a video from YouTube related to a particular medical condition. If other clients learn about the identity of that request, this may then violate the privacy of that client. In this paper, we are interested in studying how to maintain the privacy of clients sharing a broadcast domain.

It is well established that coding across the content messages of the clients is needed to efficiently use the shared broadcast domain, as formalized in index coding [1]. A typical index coding instance consists of a server with m messages, connected through a broadcast channel to a set of n clients. Each client possesses a subset of the messages as side information and

requires a specific new message. The server then uses these side information sets to send coded transmissions, which efficiently deliver the required messages to the clients.

In this paper we claim that index coding poses a privacy challenge. Consider, for example, that a server transmits $b_1 + b_2$ to satisfy client 1. Since this is a broadcast transmission, other clients observing this transmission will infer that the request of client 1 is either b_1 or b_2 , while the other message must belong to her side information. This suggests that, although the clients can securely convey their requests to the server (e.g., through pairwise keys), a curious client may be able to infer information about the requests and/or side information sets of other clients by learning the encoding matrix used to generate the broadcast transmissions.

The first question we ask is: how much information does the encoding matrix in index coding reveal about the requests and the side information of other users? At a high level, one can think of the request and side information as two shared secrets between each client and the server, where one secret could be used to protect the other. Therefore, as we also show in the paper, these two aspects exhibit a trade-off: maintaining a certain level of privacy on one aspect limits the amount of privacy level achieved on the other. We also ask: can we design index coding matrices that, for a given number of transmissions, achieve the highest possible level of privacy? How should these matrices be designed and how much privacy can they guarantee?

In this paper, we take first steps in answering such questions. Our main contributions can be summarized as follows:

- 1) We propose an information-theoretic metric to characterize the levels of privacy that can be guaranteed. We then provide guidelines for designing encoding matrices and transmission strategies to achieve high privacy levels;
- 2) We design an encoding matrix and characterize the maximum levels of privacy that it can achieve;
- 3) We derive universal upper bounds (i.e., which hold independently of the scheme that is used) on the maximum levels of privacy that can be attained;
- 4) We consider a special case of the problem and we characterize in closed-form the levels of privacy achieved by our scheme, which then we compare to the outer bounds, hence highlighting the privacy trade-off.

Related Work. In secure index coding [2], the primal goal is to design strategies such that a passive external eavesdropper – who wiretaps the communication from the server to the clients – cannot learn any information about the messages. Differently, in this work we seek to protect

clients' *privacy* against adversaries who wish to learn information about the identity of the requests and side information sets of the clients.

Recently, there has been a lot of effort trying to address privacy concerns in communication setups. For instance, a set of relevant work has considered the problem of protecting privacy of a user against a database. This problem was introduced in [3] and is known as *Private Information Retrieval* (PIR). Specifically, in PIR a client wishes to receive a specific message from a set of (possibly colluding) databases, without revealing the identity of the request. Towards this end, data request and/or storage schemes were designed [4], [5] and recently the PIR capacity was characterized [6], [7].

In cryptography, the *Oblivious Transfer* (OT) problem [8] has a close connection to PIR [9]. Specifically, in OT the goal is to protect both the privacy of the client against the server (i.e., as in PIR, the identity of the request of the client is not revealed to the server) and the privacy of the server against the client (i.e., the client learns only the requested message). OT has also been used as a primitive to build techniques for secure multi-party computation [9].

Different from these works, in this paper we seek to understand the privacy issues that can arise among clients who share the same broadcast domain. Specifically, we seek to design techniques that guarantee high levels of privacy both in the side information and in the request of a client against another curious client. Given the different problem formulation, the techniques developed to solve the PIR and OT problems do not easily extend to our setup.

Paper Organization. The paper is organized as follows. In Section II we define our setup. In Section III we provide definitions and guidelines on how to design privacy-preserving transmission schemes and we derive fundamental upper bounds. In Section IV we present the design of a privacy-preserving matrix. Based on this matrix, in Section V we consider a specific scenario for which we propose a transmission scheme and assess its performance. In Section VI we conclude the paper. Some of the proofs are delegated to the appendices.

Notation. Calligraphic letters indicate sets; boldface lower case letters denote vectors and boldface upper case letters indicate matrices; $|\mathcal{X}|$ is the cardinality of \mathcal{X} ; $[n]$ is the set of integers $\{1, \dots, n\}$; $2^{[n]}$ and $\binom{[n]}{s}$ are the power set and the set of all possible subsets of $[n]$ of size s , respectively; for all $x \in \mathbb{R}$, the floor function is denoted with $\lfloor x \rfloor$; for a sequence $X = \{X_1, \dots, X_n\}$, $X_{\mathcal{S}}$ is the subsequence of X where only the elements indexed by \mathcal{S} are retained; $\mathbf{0}_{i \times j}$ is the all-zero matrix of dimension $i \times j$; $\mathbf{A}_{\mathcal{S}}$ is the submatrix of \mathbf{A} where only the

columns indexed by \mathcal{S} are retained; $\text{span}(\mathbf{A})$ is the linear span of the columns of \mathbf{A} ; $H(X|y)$ is the entropy of the random variable X , conditioned on the *specific* realization y ; $\binom{n}{k} = 0$ if $k < 0$ or $k > n$; logarithms are in base 2.

II. SETUP

We consider a typical index coding instance, where a set of clients $\mathcal{N} = \{c_{[n]}\}$, with $|\mathcal{N}| = n$, are connected to a server through a shared broadcast channel. The server has a database of messages $\mathcal{M} = \{b_{[m]}\}$, with $|\mathcal{M}| = m$. Each client $c_i, i \in [n]$, is represented by a pair of random variables, namely: (i) $\bar{Q}_i \in [m]$ associated with the index of the message that c_i wishes to download from the server and (ii) $\bar{S}_i \in 2^{[m]}$, associated with the indices of the subset of messages she already has as side information. We indicate with \bar{q}_i and \bar{s}_i the realizations of \bar{Q}_i and \bar{S}_i , respectively, which are chosen uniformly at random from their respective domains. Clearly, $\bar{q}_i \notin \bar{S}_i$. We assume that the pairs $(\bar{Q}_i, \bar{S}_i), \forall i \in [n]$, are independent across $i \in [n]$.

Server Model. We assume that the server knows the request and the side information of each client, i.e., it is aware of the realizations of the random variables $\bar{Q}_i = \bar{q}_i$ and $\bar{S}_i = \bar{s}_i$, with $i \in [n]$. Given this, the server seeks to satisfy the requests of the clients through T broadcast transmissions. The server employs linear encoding, i.e., each transmission consists of a linear combination of the m messages, where the coefficients are chosen from a finite field \mathbb{F}_L with L being large enough. This can be mathematically formulated as $\mathbf{A}\mathbf{b} = \mathbf{y}$, where $\mathbf{b} \in \mathbb{F}_L^m$ is the column vector of the m messages, $\mathbf{A} \in \mathbb{F}_L^{T \times m}$ is the encoding matrix used by the server and $\mathbf{y} \in \mathbb{F}_L^T$ is the column vector with linear combinations of the messages.

Therefore, a *transmission scheme* employed by the server consists of the following two components:

- i) *Transmission space*: a specific set \mathcal{A} of encoding matrices designed to satisfy the clients and protect their privacy;
- ii) *Transmission strategy*: a function that, given $(\bar{q}_{[n]}, \bar{s}_{[n]})$, determines the encoding matrix $\mathbf{A} \in \mathcal{A}$ to be used. We model the output of the function as a random variable \mathbf{A} where $\mathbf{A} = \hat{\mathbf{A}}$ according to a probability distribution $p_{\mathbf{A}|\bar{Q}_{[n]}, \bar{S}_{[n]}}(\hat{\mathbf{A}}|\bar{q}_{[n]}, \bar{s}_{[n]})$ that has to be designed.

Adversary Model. We assume that some of the clients – referred to as *eavesdroppers* – are malicious. Specifically, the eavesdroppers are non-cooperative clients who, based on the broadcast transmissions they receive, are eager to infer information about the requests and the

side information sets of other clients. Since the eavesdroppers do not cooperate, without loss of generality, we can assume that there is only one eavesdropper in the system, namely client c_n . In addition, we assume that the eavesdropper c_n : (i) is aware of both the transmission scheme employed by the server and the underlying distribution based on which the clients obtain their requests and side information sets; (ii) has infinite computational power; (iii) knows the size of the side information set of each client, i.e., $s_i = |\bar{S}_i|, i \in [n]$. This last assumption, which we make to simplify the analysis, provides pessimistic privacy guarantees with respect to a scenario where the eavesdropper does not have this information.

Based on this knowledge, the eavesdropper c_n wishes to infer information about the request and side information of the other clients. Specifically, we denote with Q_i and S_i the random variables, which represent the eavesdropper's estimate of the request and side information of client c_i , respectively and we let $p_{Q_i}(q_i)$ and $p_{S_i}(s_i)$ be the corresponding probability density functions. For ease of notation, in the rest of the paper, we drop the subscripts from the probability density functions while retaining the arguments. Clearly, $Q_n = \bar{Q}_n$ and $S_n = \bar{S}_n$. Before transmission, the eavesdropper is completely oblivious to Q_i and S_i for $i \in [n-1]$; we model this situation by having $p(q_i|s_i)$ and $p(S_i|s_i)$ uniformly distributed over $[m]$ and $\binom{[m]}{s_i}$, respectively¹. Then, by learning the specific encoding matrix $\hat{\mathbf{A}}$ employed by the server, the eavesdropper infers some information about the other clients, which is reflected in the conditional probability distributions $p(q_i|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$ and $p(S_i|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$.

Privacy Metric. We consider the amount of knowledge the eavesdropper has about the variables Q_i and S_i as a privacy metric. In particular, we evaluate how far the uniform distribution is from the conditional distribution that the eavesdropper has after learning the encoding matrix $\hat{\mathbf{A}}$. Let $X \in \{Q_{[n]}, S_{[n]}\}$. Then, inspired by the t-closeness metric for data privacy [10], we consider the *Kullback–Leibler divergence* as a distance metric between the distributions $p(x|\hat{\mathbf{A}}, s_i, q_n, \mathcal{S}_n)$ and $p(x|s_i)$, namely

$$D_{\text{KL}}(p(x|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) || p(x|s_i)) = \log(|\mathcal{X}|) - H(X|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n), \quad (1)$$

where \mathcal{X} is the support of X (note that the entropy used throughout the paper is conditioned on specific realizations). If $D_{\text{KL}}(p(x|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) || p(x|s_i)) = 0$, i.e., $H(X|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) =$

¹In principle, in $p(q_i|s_i)$ and $p(S_i|s_i)$ we should also have q_n, \mathcal{S}_n and $s_{[n] \setminus \{i\}}$ in the conditioning. However, since (\bar{Q}_i, \bar{S}_i) , $\forall i \in [n]$, are independent across i , we can safely drop this dependence.

$\log(|\mathcal{X}|)$), then the eavesdropper has no knowledge of the variable X . Differently, larger values of $D_{\text{KL}}(p(x|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) || p(x|s_i))$, i.e., smaller values of $H(X|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$ indicate lower levels of privacy. Therefore, we consider $H(X|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$ as an indication of the level of privacy attained for the variable X . We focus on designing transmission schemes with guaranteed levels of privacy regarding three different quantities for each client:

- i) Privacy in the request, captured by $H(Q_i|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$;
- ii) Privacy in the side information, captured by $H(S_i|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$;
- iii) Joint privacy, captured by $H(Q_i, S_i|\hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$.

Therefore, our goal is to design a transmission scheme which provides privacy guarantees - in terms of the aforementioned metrics - for a given number of transmissions.

III. GUIDELINES FOR PROTECTING PRIVACY

Based on the knowledge of $(\bar{Q}_{[n]}, \bar{S}_{[n]})$, the server chooses to use an encoding matrix $\mathbf{A} = \hat{\mathbf{A}}$ such that it satisfies all clients, i.e., it allows each client to decode her request using her side information set.

Definition III.1. A (q, \mathcal{S}) pair is said to be *decodable in $\hat{\mathbf{A}}$* if, using $\hat{\mathbf{A}}$ as encoding matrix, message b_q can be decoded knowing $b_{\mathcal{S}}$.

Definition III.2. A q (or \mathcal{S}) is said to be *decodable in $\hat{\mathbf{A}}$* if there exists \mathcal{S} (or q) such that (q, \mathcal{S}) is decodable in $\hat{\mathbf{A}}$.

In order to design an encoding matrix that satisfies all clients, we rely on the following lemma – a slight variation of [11, Lemma 4] – which provides a decodability criterion for (q, \mathcal{S}) using a matrix $\hat{\mathbf{A}}$.

Lemma III.1 (Decodability Criterion). Let $\hat{\mathbf{A}}$ be the encoding matrix used by the server. Then, the pair (q, \mathcal{S}) is decodable in $\hat{\mathbf{A}}$ iff $\hat{\mathbf{A}}_q \notin \text{span}(\hat{\mathbf{A}}_{[m] \setminus \{q \cup \mathcal{S}\}})$.

Lemma III.1 provides a necessary and sufficient algebraic condition on whether a particular (q, \mathcal{S}) pair is decodable using a given encoding matrix. The eavesdropper, when trying to infer information about $c_i, i \in [n-1]$, can therefore apply this decodability criterion on all possible (q_i, \mathcal{S}_i) pairs with $|\mathcal{S}_i| = s_i$, to determine the subset of pairs that are decodable using $\hat{\mathbf{A}}$. In other words, since she knows that the request of client c_i must be satisfied, then the actual $(\bar{q}_i, \bar{\mathcal{S}}_i)$ pair of client c_i must belong to this set of decodable pairs. Thus, the size of the set of decodable

pairs with side information sets of size s_i determines the uncertainty that the eavesdropper has regarding the information of client c_i and hence the attained levels of privacy for c_i . Therefore, in order to maintain high levels of privacy, it is imperative to design encoding matrices with decodable sets of large sizes.

We next formalize this intuition. Towards this end, we define the following three quantities: (i) $\mathcal{D}(\hat{\mathbf{A}}, s_i)$, i.e., the set of decodable (q_i, \mathcal{S}_i) pairs in $\hat{\mathbf{A}}$ for client c_i ; (ii) $\mathcal{D}^Q(\hat{\mathbf{A}}, s_i)$, i.e., the set of decodable q_i in $\hat{\mathbf{A}}$ for client c_i , and (iii) $\mathcal{D}^S(\hat{\mathbf{A}}, s_i)$, i.e., the set of decodable \mathcal{S}_i in $\hat{\mathbf{A}}$ for client c_i . To better understand this notation, consider the following example.

Example. Consider $m = 5$, $n = 2$ and $s_1 = 1$. If the server uses $\hat{\mathbf{A}}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$ as an encoding matrix, then $\mathcal{D}(\hat{\mathbf{A}}_1, 1) = \{(1, i), (3, j)\}$ with $i \in [5] \setminus \{1\}$ and $j \in [5] \setminus \{3\}$, $\mathcal{D}^Q(\hat{\mathbf{A}}_1, 1) = \{1, 3\}$ and $\mathcal{D}^S(\hat{\mathbf{A}}_1, 1) = [5]$. Now, suppose that the server uses $\hat{\mathbf{A}}_2 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$. Then, $\mathcal{D}(\hat{\mathbf{A}}_2, 1) = \{(1, 2), (2, 1), (3, 4), (4, 3)\}$, $\mathcal{D}^Q(\hat{\mathbf{A}}_2, 1) = \mathcal{D}^S(\hat{\mathbf{A}}_2, 1) = [4]$. Clearly, $|\mathcal{D}(\hat{\mathbf{A}}_1, 1)| > |\mathcal{D}(\hat{\mathbf{A}}_2, 1)|$ and $|\mathcal{D}^S(\hat{\mathbf{A}}_1, 1)| > |\mathcal{D}^S(\hat{\mathbf{A}}_2, 1)|$, but $|\mathcal{D}^Q(\hat{\mathbf{A}}_1, 1)| < |\mathcal{D}^Q(\hat{\mathbf{A}}_2, 1)|$.

With this, we have the following remark that relates the privacy metrics to the sizes of the decodable sets (see Appendix A for details).

Remark III.2. When the eavesdropper observes the encoding matrix $\hat{\mathbf{A}}$, then for all $i \in [n - 1]$ and $s_i \in [m - 1]$, we have

$$H(Q_i, \mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) \leq \log |\mathcal{D}(\hat{\mathbf{A}}, s_i)|, \quad (2a)$$

$$H(Q_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) \leq \log |\mathcal{D}^Q(\hat{\mathbf{A}}, s_i)|, \quad (2b)$$

$$H(\mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) \leq \log |\mathcal{D}^S(\hat{\mathbf{A}}, s_i)|. \quad (2c)$$

Moreover, these bounds are tight iff the corresponding probability distributions are uniform. Namely:

- i) eq.(2a) is tight iff $p(q_i, \mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$ is uniform over $(q_i, \mathcal{S}_i) \in \mathcal{D}(\hat{\mathbf{A}}, s_i)$;
- ii) eq.(2b) is tight iff $p(q_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$ is uniform over $q_i \in \mathcal{D}^Q(\hat{\mathbf{A}}, s_i)$;
- iii) eq.(2c) is tight iff $p(\mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$ is uniform over $\mathcal{S}_i \in \mathcal{D}^S(\hat{\mathbf{A}}, s_i)$.

Remark III.2 implies that the sizes of the decodable sets give an upper bound on the corresponding levels of the privacy metrics. Moreover, one can show that the conditions i) to iii) in Remark III.2 hold – and hence bounds (2a) to (2c) are tight – if $p(\hat{\mathbf{A}} | \bar{q}_{[n]}, \bar{\mathcal{S}}_{[n]})$ in the transmission

strategy (described in Section II) is properly designed. For instance, using Bayes' rule, it can be shown – see Appendix A for the details – that condition i) is satisfied iff

$$\sum_{q_{\mathcal{K}}, \mathcal{S}_{\mathcal{K}} \in \prod_{j \in \mathcal{K}} \mathcal{D}(\hat{\mathbf{A}}, s_j)} p(\hat{\mathbf{A}} | q_{[n]}, \mathcal{S}_{[n]}, s_{[n]}), \quad \mathcal{K} = [n-1] \setminus \{i\}$$

is the same for all $(q_i, \mathcal{S}_i) \in \mathcal{D}(\hat{\mathbf{A}}, s_i)$.

From Remark III.2, it follows that the design of privacy-preserving transmission schemes consists of two main steps: (i) designing encoding matrices with large decodable sets and (ii) using transmission strategies which satisfy uniformity conditions and hence achieve maximum levels of privacy.

Based on the result in Remark III.2, we now derive universal upper bounds (i.e., which hold independently of the encoding matrix that the server uses) on the decodable sets and hence on the levels of the privacy metrics. In particular, we have

Lemma III.3. For any $\hat{\mathbf{A}} \in \mathbb{F}_L^{T \times m}$ and $s_i \in [m-1]$, we have

$$|\mathcal{D}(\hat{\mathbf{A}}, s_i)| \leq T \binom{m}{s_i} =: \text{UB}_{Q,S}, \quad (3a)$$

$$|\mathcal{D}^Q(\hat{\mathbf{A}}, s_i)| \leq m =: \text{UB}_Q, \quad (3b)$$

$$|\mathcal{D}^S(\hat{\mathbf{A}}, s_i)| \leq \binom{m}{s_i} =: \text{UB}_S. \quad (3c)$$

Proof: The upper bounds in (3b) and (3c) simply follow by noticing that the size of a decodable set is upper bounded by the size of the support of the corresponding random variable. We next prove the bound in (3a). For a given encoding matrix $\hat{\mathbf{A}} \in \mathbb{F}_L^{T \times m}$, one can write $\mathcal{D}(\hat{\mathbf{A}}, s_i) = \sum_{\mathcal{S}_i \in \binom{[m]}{s_i}} \mathcal{N}(\hat{\mathbf{A}}, \mathcal{S}_i)$, where $\mathcal{N}(\hat{\mathbf{A}}, \mathcal{S}_i)$ is the set of requests $q_i \in \mathcal{D}^Q(\hat{\mathbf{A}}, s_i)$ for which the pair (q_i, \mathcal{S}_i) is decodable. According to Lemma III.1, for each $q_i \in \mathcal{N}(\hat{\mathbf{A}}, \mathcal{S}_i)$, $\hat{\mathbf{A}}_{q_i}$ is not in the span of $\hat{\mathbf{A}}_{[m] \setminus \mathcal{S}_i \cup q_i}$. It is therefore straightforward to show that the columns of $\hat{\mathbf{A}}_{\mathcal{N}(\hat{\mathbf{A}}, \mathcal{S}_i)}$ are linearly independent. Thus, $|\mathcal{N}(\hat{\mathbf{A}}, \mathcal{S}_i)| \leq T$ and hence we have $|\mathcal{D}(\hat{\mathbf{A}}, s_i)| \leq T \binom{m}{s_i}$. ■

IV. DESIGN OF A TRANSMISSION SPACE

In this section, we take first steps towards designing a privacy-preserving transmission scheme. Specifically, we design an encoding matrix, referred to as the *base* matrix \mathbf{A}^{base} . Then, we populate the transmission space with the matrices obtained from \mathbf{A}^{base} by taking all the permutations of its columns. Our design of \mathbf{A}^{base} is based on the use of Maximum Distance Separable

$$\begin{array}{cccc}
\text{Seg. 1} & \text{Seg. 2} & & \text{Seg. } k & \text{Seg. 0} \\
\hline
\begin{bmatrix} \mathbf{A}_b \\ \mathbf{0}_{\frac{T}{k} \times \ell} \\ \vdots \\ \mathbf{0}_{\frac{T}{k} \times \ell} \end{bmatrix} & \begin{bmatrix} \mathbf{0}_{\frac{T}{k} \times \ell} \\ \mathbf{A}_b \\ \vdots \\ \mathbf{0}_{\frac{T}{k} \times \ell} \end{bmatrix} & \begin{bmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix} & \begin{bmatrix} \mathbf{0}_{\frac{T}{k} \times \ell} \\ \mathbf{0}_{\frac{T}{k} \times \ell} \\ \vdots \\ \mathbf{A}_b \end{bmatrix} & \mathbf{0}_{T \times m - k\ell}
\end{array}$$

Figure 1. Design of the base matrix \mathbf{A}^{base} for the achievable scheme.

(MDS) codes. A generator matrix of an $[m, T]$ MDS code has the property that any $T \times T$ submatrix is full rank, i.e., any T columns are linearly independent. Such matrices promise to provide large decodable sets. To see this notice that, for a given side information set \mathcal{S} with $|\mathcal{S}| \geq m - T$, all requests in $[m] \setminus \mathcal{S}$ are decodable with \mathcal{S} . Therefore, if $\mathbf{B} \in \mathbb{F}_L^{T \times m}$ is a generator matrix of an $[m, T]$ MDS code, then, for all $s \geq m - T$, we have $|\mathcal{D}^Q(\mathbf{B}, s)| = m$ and $|\mathcal{D}(\mathbf{B}, s)| = m \binom{m-1}{s} = O(m^s)$. However, this scheme might require a prohibitively large number of transmissions T , especially when m is large and s is small compared to m . To achieve high levels of privacy with T that is not that large, we next propose the design of \mathbf{A}^{base} , which is based on a block-MDS as shown in Figure 1 and structured as follows:

- i) The columns of \mathbf{A}^{base} are divided in $k + 1$ segments, labeled as “Seg. 0 to k ”, where T is a multiple of k ;
- ii) Segments from 1 to k consist of ℓ columns, where $\ell \leq \min\{s_{\min} + T/k, \lfloor m/k \rfloor\}$, with $s_{\min} = \min_{i \in [n]} s_i$;
- iii) A matrix $\mathbf{A}_b \in \mathbb{F}_L^{\frac{T}{k} \times \ell}$ is constructed as the generator matrix of an $[\ell, T/k]$ MDS code; then, \mathbf{A}_b is repeated k times and positioned in \mathbf{A}^{base} as shown in Figure 1;
- iv) The rest of \mathbf{A}^{base} is filled with zeros.

Note that, for any number of clients n and messages m , one can always find values of k , ℓ and T so that \mathbf{A}^{base} satisfies all clients (e.g., $k = 1$, $\ell = s_{\min}$ and $T = n$).

We now analyze the performance of our proposed \mathbf{A}^{base} in terms of the sizes of its decodable sets (see Appendix B). These, by means of Remark III.2, provide upper bounds on the levels of privacy that could be attained using \mathbf{A}^{base} .

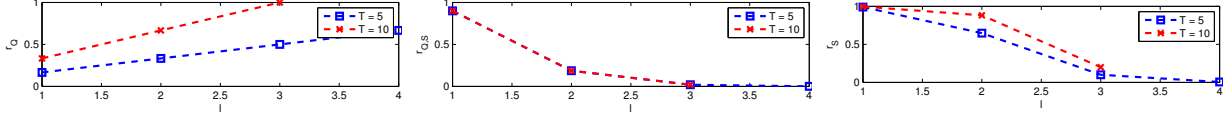


Figure 2. Numerical evaluation of r_Q , r_S and $r_{Q,S}$ - $m = 30$ and $s = 3$.

Theorem IV.1. For \mathbf{A}^{base} and any $s_i \in [m - 1]$, we have

$$H(Q_i, S_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) \leq \log \left(k\ell \sum_{j=\ell-T/k}^{\ell-1} \binom{\ell-1}{j} \binom{m-\ell}{s_i-j} \right), \quad (4a)$$

$$H(Q_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) \leq (k\ell). \quad (4b)$$

where the bounds can be achieved by satisfying the uniformity conditions in Remark III.2

In the next section we study a special scenario in which we use the transmission space here proposed (i.e., populated by the matrices obtained from \mathbf{A}^{base} by taking all the permutations of its columns) and we design the transmission strategy.

V. TRANSMISSION STRATEGY FOR A SPECIAL CASE

In the previous section, we designed a transmission space that consists of all possible matrices obtained by permuting the columns of the matrix \mathbf{A}^{base} . Thus, as discussed in Section II, in order to design a transmission scheme, we need to design a transmission strategy that selects which specific matrix to use according to a probability distribution. However, designing such a transmission strategy that achieves the upper bounds in Remark III.2 is non-trivial. To get an analytical handle on the problem, we take a first step and consider a simplified model: we assume $n = 2$ and an eavesdropper who does *not* have a request. Such a scenario can model a situation where the $n = 2$ clients (the second of which is the eavesdropper) do not have a simultaneous request.

Since only one client needs to be satisfied, then we can use our proposed encoding matrix \mathbf{A}^{base} with $k = T$ and $\ell \leq \min\{s_1 + 1, \lfloor m/T \rfloor\}$, knowing that the client c_1 can always be satisfied by using the appropriate column-permutation of \mathbf{A}^{base} (i.e., by ensuring that $\mathbf{A}_{q_1}^{\text{base}}$ is non-zero, and all other columns belonging to the same segment of $\mathbf{A}_{q_1}^{\text{base}}$ correspond to messages in \mathcal{S}_1). In this case, \mathbf{A}_b is a row vector of arbitrary non-zero values. The following theorem (whose proof can be found in Appendix C) then provides analytical guarantees on the attained performance of this scheme.

Theorem V.1. For the scheme described above, we have

$$H(Q_1, S_1 | \hat{\mathbf{A}}, s_1) = \log T \ell \binom{m - \ell}{s_1 - \ell + 1} =: \text{LB}_{Q,S}, \quad (5a)$$

$$H(Q_1 | \hat{\mathbf{A}}, s_1) = \log T \ell =: \text{LB}_Q, \quad (5b)$$

$$H(S_1 | \hat{\mathbf{A}}, s_1) = \log T \ell \binom{m - \ell}{s_1 - \ell + 1} - \text{K} =: \text{LB}_S, \quad (5c)$$

$$\text{K} = \sum_{i=1}^T \binom{T-1}{i-1} \ell^{i-1} \frac{\binom{m-i\ell}{s_1-i(\ell-1)}}{\binom{m-\ell}{s_1-\ell+1}} \sum_{x=1}^i (-1)^{i-x} \binom{i-1}{x-1} \log x,$$

where $\hat{\mathbf{A}}$ is the column permutation of \mathbf{A}^{base} that is used.

Note that the two quantities in (5a) and (5b) meet the upper bounds that follow from Theorem IV.1 by applying the conditions in Remark III.2. Moreover, in order to get the bounds in (5), we used a transmission strategy for which $p(\hat{\mathbf{A}} | \bar{q}_1, \bar{S}_1)$ is uniform over all $\hat{\mathbf{A}}$ that satisfy (\bar{q}_1, \bar{S}_1) for all $(\bar{q}_1, \bar{S}_1) \in \mathcal{D}(\hat{\mathbf{A}}, s_1)$. This is because, thanks to the special structure of \mathbf{A}^{base} , the number of column-permutations of \mathbf{A}^{base} that satisfies a given (\bar{q}_1, \bar{S}_1) is equal for all (\bar{q}_1, \bar{S}_1) .

We next analyze the performance of our scheme. Towards this end, we define the following quantities:

- $G_{Q,S} := \log(\text{UB}_{Q,S}) - \text{LB}_{Q,S}$, $r_{Q,S} = 2^{-G_{Q,S}}$;
- $G_Q := \log(\text{UB}_Q) - \text{LB}_Q$, $r_Q = 2^{-G_Q}$;
- $G_S := \log(\text{UB}_S) - \text{LB}_S$, $r_S = 2^{-G_S}$.

Figure 2 shows an example of how the quantities $r_{Q,S}$, r_Q and r_S behave as ℓ changes. Note that all these quantities are fractions and hence the maximum level of privacy (y-axis) is 1. Figure 2 shows that as ℓ increases, higher values of privacy are attained in the requests (i.e., r_Q increases), but smaller levels of privacy are achieved in the side information (i.e., r_S decreases). This highlights a trade-off: maintaining a certain level of privacy on one aspect limits the amount of privacy level achieved on the other. It is also noted that increasing T increases the attained values of r_Q and r_S for the same value of ℓ . We believe that the reason such increase does not occur in $r_{Q,S}$ is because $\text{UB}_{Q,S}$ in (3a) is loose.

Next, we assess the performance of our scheme when the parameters of the system grow. We assume that $s_1 = c \cdot m$ and $\ell = b \cdot m + 1$, where $b \leq c \leq \frac{m-1}{m}$. We consider two cases:

Case I: $c = \frac{m-k_c}{m}$ **where $k_c > 0$ is a constant.** In this case, full privacy in the request, side information and their joint can be achieved by using an $[m, T]$ MDS code with $T = k_c$.

Case II: c and T are constants. In this case, by choosing $b = 0$, we get $G_Q = \log \frac{m}{T} = O(\log m)$ and $G_{Q,S} = \log \frac{\binom{m}{cm}}{T \binom{m-1}{cm}} = \log \frac{1}{T(1-c)} = O(1)$. Also, since conditioning reduces the entropy, we have $H(S_1|\hat{\mathbf{A}}, s_1) \geq \text{eq. (5a)} - \text{eq. (5b)}$, which implies $G_S \leq \log \frac{\binom{m}{cm}}{\binom{m-1}{cm}} = \log \frac{1}{1-c} = O(1)$. This suggests that when s_1 grows as a constant fraction of m , then with a constant number of transmissions we can have almost perfect side information (and joint) privacy, but very little privacy in the request. However, if we choose $b = c$, then we get $G_Q \leq \log \frac{1}{Tc} = O(1)$, $G_{Q,S} = G_S \leq \log \binom{m}{cm} = O(m \log m)$ since, under these conditions, $K = 0$ in (5c). Thus, in this case almost full privacy is achieved in the request while very little privacy is attained in the side information (and in the joint).

VI. CONCLUSION

We considered an index coding instance where some clients are malicious: they wish to learn information about the requests and side information of the other clients. We showed how this privacy breach is possible by learning the encoding matrix used by the server. We proposed information-theoretic metrics to model the levels of privacy that can be guaranteed and we designed an encoding matrix for protecting privacy. Then, for a special case of the problem, we derived in closed-form the levels of privacy that our proposed scheme achieves. We showed an inherent trade-off between protecting privacy of either the request or the side information set of the clients.

REFERENCES

- [1] Z. Bar-Yossef, Y. Birk, T. Jayram, and T. Kol, "Index coding with side information," *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1479–1494, Mar. 2011.
- [2] S. H. Dau, V. Skachek, and Y. M. Chee, "On the security of index coding with side information," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3975–3988, Jun. 2012.
- [3] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *Journal of the ACM (JACM)*, vol. 45, no. 6, pp. 965–981, Nov. 1998.
- [4] R. Tajeddine and S. E. Rouayheb, "Private information retrieval from MDS coded data in distributed storage systems," *arXiv:1602.01458*, Feb. 2016.
- [5] R. Freij-Hollanti, O. Gnille, C. Hollanti, and D. Karpuk, "Private information retrieval from coded databases with colluding servers," *arXiv:1611.02062*, Nov. 2016.
- [6] H. Sun and S. A. Jafar, "The capacity of private information retrieval," *arXiv:1602.09134*, Feb. 2016.
- [7] K. Banawan and S. Ulukus, "The capacity of private information retrieval from coded databases," *arXiv:1609.08138*, Sep. 2016.

- [8] G. Brassard, C. Crepeau, and J.-M. Robert, “All-or-nothing disclosure of secrets,” *Advances in Cryptology: Proceedings of Crypto '86*, Springer-Verlag, pp. 234–238, 1987.
- [9] M. Mishra, B. K. Dey, V. M. Prabhakaran, and S. Diggavi, “The oblivious transfer capacity of the wiretapped binary erasure channel,” in *IEEE International Symposium on Information Theory*, Jun. 2014, pp. 1539–1543.
- [10] N. Li, T. Li, and S. Venkatasubramanian, “t-closeness: Privacy beyond k-anonymity and l-diversity,” in *IEEE 23rd International Conference on Data Engineering*, Apr. 2007, pp. 106–115.
- [11] L. Song and C. Fragouli, “Content-type coding,” in *International Symposium on Network Coding (NetCod)*, Jun. 2015, pp. 31–35.

APPENDIX A

We prove the result for the upper bound in (2a). Given $\hat{\mathbf{A}}$ and s_i , the set $\mathcal{D}(\hat{\mathbf{A}}, s_i)$ consists of all possible (q_i, \mathcal{S}_i) pairs that could be the request/side information pair for c_i . Therefore, $p(q_i, \mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) = 0$ for all $(q_i, \mathcal{S}_i) \notin \mathcal{D}(\hat{\mathbf{A}}, s_i)$. Therefore,

$$H(Q_i, \mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) = - \sum_{(q_i, \mathcal{S}_i) \in \mathcal{D}(\hat{\mathbf{A}}, s_i)} p(q_i, \mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) \log p(q_i, \mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) \leq \log |\mathcal{D}(\hat{\mathbf{A}}, s_i)|,$$

thus proving (2a). Since $p(q_i, \mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) = 0$ for all $(q_i, \mathcal{S}_i) \notin \mathcal{D}(\hat{\mathbf{A}}, s_i)$, then this upper bound is achieved if and only if $p(q_i, \mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n)$ is uniform over for $(q_i, \mathcal{S}_i) \in \mathcal{D}(\hat{\mathbf{A}}, s_i)$, thus proving the uniformity condition *i*) on (2a). Similar arguments can be made to prove (2b) and (2c).

Next, we show that the uniformity conditions in *i*)-*iii*) imply constraints on the design of the transmission strategy $p(\hat{\mathbf{A}} | q_{[n]}, \mathcal{S}_{[n]})$. To see this, note that we can write

$$p(q_i, \mathcal{S}_i | \hat{\mathbf{A}}, s_{[n]}, q_n, \mathcal{S}_n) = p(\hat{\mathbf{A}} | q_{\{i,n\}}, \mathcal{S}_{\{i,n\}}, s_{[n]}) \frac{p(q_i, \mathcal{S}_i | s_{[n]}, q_n, \mathcal{S}_n)}{p(\hat{\mathbf{A}} | s_{[n]}, q_n, \mathcal{S}_n)},$$

which follows by applying Bayes' rule. Since the probabilities in the fraction term do not depend on the value of (q_i, \mathcal{S}_i) (note that $p(q_i, \mathcal{S}_i | s_{[n]})$ is uniform), then the uniformity condition *i*) is satisfied if and only if the term $p(\hat{\mathbf{A}} | q_{\{i,n\}}, \mathcal{S}_{\{i,n\}}, s_{[n]})$ is the same for all $(q_i, \mathcal{S}_i) \in \mathcal{D}(\hat{\mathbf{A}}, s_i)$. We can further write

$$p(\hat{\mathbf{A}} | q_{\{i,n\}}, \mathcal{S}_{\{i,n\}}, s_{[n]}) = \sum_{q_{\mathcal{K}}, \mathcal{S}_{\mathcal{K}} \in \prod_{j \in \mathcal{K}} \mathcal{D}(\hat{\mathbf{A}}, s_j)} p(\hat{\mathbf{A}} | q_{[n]}, \mathcal{S}_{[n]}, s_{[n]}) p(q_{\mathcal{K}}, \mathcal{S}_{\mathcal{K}} | q_i, \mathcal{S}_i, s_{[n]}), \quad \mathcal{K} = [n-1] \setminus i.$$

Note that the distribution $p(q_{\mathcal{K}}, \mathcal{S}_{\mathcal{K}} | q_i, \mathcal{S}_i, s_{[n]})$ is assumed to be uniform and independent over $i \in [n]$. Therefore, to satisfy the uniformity condition, we must have the summation term on the

Righ-Hand Side to be the same for all $(q_i, \mathcal{S}_i) \in \mathcal{D}(\hat{\mathbf{A}}, s_i)$. This therefore imposes constraints on the transmission strategy used by the server. We can similarly show that the uniformity conditions on (2b) and (2c) also impose constraints on the used transmission strategy.

APPENDIX B

In order to prove Theorem IV.1, we need to characterize the quantities $|\mathcal{D}(\hat{\mathbf{A}}, s)|$ and $|\mathcal{D}^Q(\hat{\mathbf{A}}, s)|$, and therefore, using Remark III.2 the result in Theorem IV.1 follows.

Characterizing $|\mathcal{D}^Q(\hat{\mathbf{A}}, s)|$: One can show that every request q whose corresponding column $\mathbf{A}_q^{\text{base}}$ is non-zero has at least one side information set \mathcal{S} with which (q, \mathcal{S}) is decodable in \mathbf{A}^{base} . If this in fact is true, then the result $|\mathcal{D}^Q(\mathbf{A}^{\text{base}}, s)| = k\ell$ follows immediately, since we have $k\ell$ such requests. To prove this statement then, notice that $\ell \leq s_{\min} + T/k$. Then consider a side information set with $|\mathcal{S}| = s_{\min}$ and where all the elements of \mathcal{S} correspond to columns of the same segment as $\mathbf{A}_q^{\text{base}}$. Therefore, the set of all columns of \mathbf{A}^{base} belonging to the same segment as $\mathbf{A}_q^{\text{base}}$ and do not belong to \mathcal{S} is of size $\ell - |\mathcal{S}| = T/k$. They are therefore linearly independent, and q is decodable with \mathcal{S} .

Characterizing $|\mathcal{D}(\hat{\mathbf{A}}, s)|$: To prove the remaining quantity, notice that we can write $\mathcal{D}(\mathbf{A}^{\text{base}}, s) = \sum_{q \in [m]} \mathcal{N}(\mathbf{A}^{\text{base}}, q)$, where $\mathcal{N}(\mathbf{A}^{\text{base}}, q)$ is the number of side information sets that are decodable with q in \mathbf{A}^{base} . For a given q , this quantity is equal to

$$\mathcal{N}(\mathbf{A}^{\text{base}}, q) = \sum_{i=\ell-T/k}^{\ell-1} \binom{\ell-1}{i} \binom{m-\ell}{s-i}, \quad (6)$$

for all q with $\mathbf{A}_q^{\text{base}}$ being non-zero, and 0 otherwise. Since this quantity does not depend on the value of q , then the result follows that $\mathcal{D}(\mathbf{A}^{\text{base}}, s) = k\ell \sum_{i=\ell-T/k}^{\ell-1} \binom{\ell-1}{i} \binom{m-\ell}{s-i}$. What remains is to prove (6), which we justify as follows: Consider a given q with a non-zero corresponding column in \mathbf{A}^{base} , and let j be the index of the segment to which $\mathbf{A}_q^{\text{base}}$ belongs. For a given side information set \mathcal{S} , let i be the number of elements in \mathcal{S} whose corresponding columns in \mathbf{A}^{base} belong to j . Then, (q, \mathcal{S}) is decodable in \mathbf{A}^{base} if and only if the elements $\ell - T/k \leq i \leq \ell - 1$; the lower bound is to ensure that the columns of \mathbf{A}^{base} belonging to segment j that fall outside of \mathcal{S} are linearly independent, and the upper bound is to ensure that q is not in \mathcal{S} . The number of subsets \mathcal{S} with i columns in segment j is equal to $\binom{\ell-1}{i} \binom{m-\ell}{s-i}$. Therefore, by summing over all possible i and multiplying by the number of possible requests we get the expression in (6).

APPENDIX C

For this scheme, we can have $p(\hat{\mathbf{A}}|q_1, \mathcal{S}_1) = 1/K$ for all $\hat{\mathbf{A}} \in \mathcal{A}$ for all $(q_1, \mathcal{S}_1) \in \mathcal{D}(\hat{\mathbf{A}}, s_1)$, where K is equal to

$$K = T \binom{s}{\ell-1} \underbrace{\binom{m-\ell}{\ell \ell \dots \ell}}_{k-1}^{(M)},$$

where the last term is a multinomial coefficient. This is because the number of column-permutations of $\hat{\mathbf{A}}^{\text{base}}$ that satisfies a given (q_1, \mathcal{S}_1) is equal to K , independently of the value of (q_1, \mathcal{S}_1) . This statement can be justified as follows: for a pair to be decodable, the column of the encoding matrix corresponding to q should be non-zero, and since we have T segments, then there are T possibilities for that column; thus the term T in the expression. Next, all remaining $\ell - 1$ columns of the same segment must correspond to elements in the side information set; thus the term $\binom{s}{\ell-1}$. Finally, among the remaining $m - \ell$ columns, we have to choose $k - 1$ segments, each of length ℓ ; thus the final multinomial term.

Calculating $H(Q_1, S_1|\hat{\mathbf{A}}, s_1)$: Note that by using the transmission strategy described above, we satisfy the uniformity condition of Remark III.2 for (2a). Therefore, we have $H(Q_1, S_1|\hat{\mathbf{A}}, s_1) = \log |\mathcal{D}(\hat{\mathbf{A}}, s_1)| = \log Tl \binom{m-\ell}{s-\ell+1}$. The last equality can be obtained by considering (4b) with $k = T$.

Calculating $H(Q_1|\hat{\mathbf{A}}, s_1)$: Using the transmission strategy described above also satisfies the uniformity condition of Remark III.2 for (2b). To see this, note that

$$p(q_1|\hat{\mathbf{A}}, s_1) = \sum_{\mathcal{S}_1: (q_1, \mathcal{S}_1) \in \mathcal{D}(\hat{\mathbf{A}}, s_1)} p(q_1, \mathcal{S}_1|\hat{\mathbf{A}}, s_1),$$

where the number of elements in the summation corresponds to the number of subsets \mathcal{S}_1 that are decodable with q_1 , which is equal to $\binom{m-\ell}{s-\ell+1}$ irrespective of q_1 . Therefore, $p(q_1|\hat{\mathbf{A}}, s_1)$ is uniform over all $q_1 \in \mathcal{D}^Q(\hat{\mathbf{A}}, s_1)$. Thus we have $H(Q_1|\hat{\mathbf{A}}, s_1) = \log |\mathcal{D}^Q(\hat{\mathbf{A}}, s_1)| = \log Tl$, where the last equality similarly holds by considering (4b) with $k = T$.

Calculating $H(S_1|\hat{\mathbf{A}}, s_1)$: Using the transmission strategy above does not satisfy the uniformity condition of Remark III.2 for (2c). Therefore, we now seek to quantify the achieved value of $H(S_1|\hat{\mathbf{A}}, s_1)$.

Note that the used transmission strategy would yield $p(q_1, \mathcal{S}_1|\hat{\mathbf{A}}, s_1) = 1/|\mathcal{D}(\hat{\mathbf{A}}, s_1)|$ for all $(q_1, \mathcal{S}_1) \in \mathcal{D}(\hat{\mathbf{A}}, s_1)$ and 0 otherwise. One can then write the marginal $p(\mathcal{S}_1|\hat{\mathbf{A}}, s_1)$ as

$$p(\mathcal{S}_1|\hat{\mathbf{A}}, s) = \sum_{q_1 \in \mathcal{D}^Q(\hat{\mathbf{A}}, s_1)} p(q_1, \mathcal{S}_1|\hat{\mathbf{A}}, s_1) = \frac{N_{\hat{\mathbf{A}}, \mathcal{S}_1}}{|\mathcal{D}(\hat{\mathbf{A}}, s_1)|},$$

where $N_{\hat{\mathbf{A}}, \mathcal{S}_1}$ is the number of requests q_1 that are decodable with \mathcal{S}_1 in $\hat{\mathbf{A}}$. Therefore, we have

$$\begin{aligned} H(\mathcal{S}_1|\hat{\mathbf{A}}, s_1) &= - \sum_{\mathcal{S}_1 \in \mathcal{D}^S(\hat{\mathbf{A}}, s_1)} \frac{N_{\hat{\mathbf{A}}, \mathcal{S}_1}}{|\mathcal{D}(\hat{\mathbf{A}}, s_1)|} \log \frac{N_{\hat{\mathbf{A}}, \mathcal{S}_1}}{|\mathcal{D}(\hat{\mathbf{A}}, s_1)|} \\ &= \log |\mathcal{D}(\hat{\mathbf{A}}, s_1)| - \underbrace{\frac{1}{|\mathcal{D}(\hat{\mathbf{A}}, s_1)|} \sum_{\mathcal{S}_1 \in \mathcal{D}^S(\hat{\mathbf{A}}, s_1)} N_{\hat{\mathbf{A}}, \mathcal{S}_1} \log N_{\hat{\mathbf{A}}, \mathcal{S}_1}}_{\bar{N}_t}. \end{aligned} \quad (7)$$

Next we calculate \bar{N}_t . For a given \mathcal{S}_1 , let $\ell_j, j \in [T]$ be the number of elements of \mathcal{S}_1 for which the corresponding columns in $\hat{\mathbf{A}}$ belong to segment j . Then in order for a pair (q_1, \mathcal{S}_1) to be decodable, then ℓ_j must be exactly equal to $\ell - 1$, where j corresponds to the segment to which $\hat{\mathbf{A}}_q$ belongs.

Note that $N_{\hat{\mathbf{A}}, \mathcal{S}_1}$ only depends on the values of ℓ_j , and therefore all subsets \mathcal{S}_1 for which $\ell_j, j \in [T]$ are the same will have the same value for $N_{\hat{\mathbf{A}}, \mathcal{S}_1}$. Based on this fact, we can then write

$$\begin{aligned} \bar{N}_t &= \sum_{\ell_1=0}^{\ell} \cdots \sum_{\ell_T=0}^{\ell} \binom{\ell}{\ell_1} \cdots \binom{\ell}{\ell_T} \binom{m - T\ell}{s_1 - \sum_{i=1}^T \ell_i} \left(\sum_{i=1}^T \mathbb{1}_{\{\ell_i = \ell-1\}} \right) \log \left(\sum_{i=1}^T \mathbb{1}_{\{\ell_i = \ell-1\}} \right) \\ &\stackrel{(a)}{=} \sum_{x=1}^T x \log x \binom{T}{x} \ell^x \overbrace{\left[\sum_{\substack{\ell_1=0 \\ \ell_1 \neq \ell-1}}^{\ell} \cdots \sum_{\substack{\ell_{T-x}=0 \\ \ell_{T-x} \neq \ell-1}}^{\ell} \binom{\ell}{\ell_1} \cdots \binom{\ell}{\ell_{T-x}} \binom{m - T\ell}{s_1 - x(\ell-1) - \sum_{i=1}^{T-x} \ell_i} \right]}^{C_{s_1, T}(T-x)} \end{aligned} \quad (8)$$

where (a) can be justified as follows: note that the possible values to which the term $\sum_{i=1}^T \mathbb{1}_{\{\ell_i = \ell-1\}}$ evaluates are $x \in [T]$ ($x = 0$ is also possible, but trivial). Moreover, it is equal to x if and only if there are exactly x indices from the set $\ell_{[T]}$ which are equal to $\ell - 1$, while the remaining indices can take any value (except $\ell - 1$). Therefore, by means of counting arguments, \bar{N}_t can be expressed as (8).

Note that we can write

$$\begin{aligned}
C_{s_1, T}(T-x) &= \left[\sum_{\substack{\ell_1=0 \\ \ell_1 \neq \ell-1}}^{\ell} \cdots \sum_{\substack{\ell_{T-x}=0 \\ \ell_{T-x} \neq \ell-1}}^{\ell} \binom{\ell}{\ell_1} \cdots \binom{\ell}{\ell_{T-x}} \binom{m-T\ell}{s_1 - x(\ell-1) - \sum_{i=1}^{T-x} \ell_i} \right] \\
&\quad \overbrace{\phantom{\sum_{\ell_1=0}^{\ell} \cdots \sum_{\ell_{T-x}=0}^{\ell} \binom{\ell}{\ell_1} \cdots \binom{\ell}{\ell_{T-x}} \binom{m-T\ell}{s_1 - x(\ell-1) - \sum_{i=1}^{T-x} \ell_i}}}^{B_{s_1, T}(T-x)} \\
&\stackrel{(b)}{=} \left[\sum_{\ell_1=0}^{\ell} \cdots \sum_{\ell_{T-x}=0}^{\ell} \binom{\ell}{\ell_1} \cdots \binom{\ell}{\ell_{T-x}} \binom{m-T\ell}{s_1 - x(\ell-1) - \sum_{i=1}^{T-x} \ell_i} \right] - \\
&\quad \sum_{y=1}^{T-x} \binom{T-x}{y} \ell^y \left[\sum_{\substack{\ell_1=0 \\ \ell_1 \neq \ell-1}}^{\ell} \cdots \sum_{\substack{\ell_{T-x-y}=0 \\ \ell_{T-x-y} \neq \ell-1}}^{\ell} \binom{\ell}{\ell_1} \cdots \binom{\ell}{\ell_{T-x-y}} \binom{m-T\ell}{s_1 - (x+y)(\ell-1) - \sum_{i=1}^{T-x-y} \ell_i} \right] \\
&= B_{s_1, T}(T-x) - \sum_{y=1}^{T-x} \binom{T-x}{y} \ell^y C_{s_1, T}(T-x-y) \tag{9}
\end{aligned}$$

where (b) follows by adding the missing summation terms of $C_{s_1, T}(T-x)$ corresponding to $\ell_i = \ell-1$ and - by means of counting - subtracting them. By noting that $C_{s_1, T}(0) = \binom{m-T\ell}{s_1-T(\ell-1)}$, equation (9) then defines a linear recurrence relation on $C_{s_1, T}(T-x)$ which we solve in the following lemma.

Lemma C.1. The solution to the linear recurrence relation in (9) is

$$C_{s_1, T}(T-x) = \sum_{v=0}^{T-x} (-1)^v \ell^v \binom{T-x}{v} B_{s_1, T}(T-x-v) \tag{10}$$

where $B_{s_1, T}(0) = \binom{m-T\ell}{s_1-T(\ell-1)}$.

Proof: We will solve the recurrence relation using strong induction. Specifically, assume that

$$C_{s_1, T}(T-x-y) = \sum_{v=0}^{T-x-y} (-1)^v \ell^v \binom{T-x-y}{v} B_{s_1, T}(T-x-y-v)$$

for $1 \leq y \leq T-x$. Then consider

$$\begin{aligned}
& \sum_{y=1}^{T-x} \binom{T-x}{y} \ell^y C_{s_1, T}(T-x-y) = \\
&= \sum_{y=1}^{T-x} \sum_{v=0}^{T-x-y} (-1)^v \ell^{v+y} \binom{T-x}{y} \binom{T-x-y}{v} B_{s_1, T}(T-x-v-y) \\
&\stackrel{(c)}{=} \sum_{k=1}^{T-x} (-1)^k \ell^k \binom{T-x}{k} B_{s_1, T}(T-x-k) \sum_{v=0}^{k-1} (-1)^{v-k} \frac{\binom{T-x}{k-v} \binom{T-x-k+v}{v}}{\binom{T-x}{k}} \\
&= \sum_{k=1}^{T-x} (-1)^k \ell^k \binom{T-x}{k} B_{s_1, T}(T-x-k) \sum_{v=0}^{k-1} (-1)^{k-v} \binom{k}{k-v} \\
&= \sum_{k=1}^{T-x} (-1)^k \ell^k \binom{T-x}{k} B_{s_1, T}(T-x-k) \sum_{v'=1}^k (-1)^{v'} \binom{k}{v'} \\
&= \sum_{k=1}^{T-x} (-1)^k \ell^k \binom{T-x}{k} B_{s_1, T}(T-x-k) (\delta_{k0} - 1) \\
&= - \sum_{k=0}^{T-x} (-1)^k \ell^k \binom{T-x}{k} B_{s_1, T}(T-x-k) + B_{s_1, T}(T-x)
\end{aligned}$$

where (c) follows by i) changing summation variables as $v + y = k$ and ii) multiplying and dividing by $(-1)^k \binom{T-x}{k}$, and where δ_{ij} is the Kronecher delta function. Therefore we have

$$\begin{aligned}
C_{s_1, T}(T-x) &= \sum_{k=0}^{T-x} (-1)^k \ell^k \binom{T-x}{k} B_{s_1, T}(T-x-k) \\
&= B_{s_1, T}(T-x) - \sum_{y=1}^{T-x} \binom{T-x}{y} \ell^y C_{s_1, T}(T-x-y)
\end{aligned}$$

satisfying (9), thus completing the proof. ■

By plugging (10) in (8), we can further simply (8) as follows

$$\begin{aligned}
\bar{N}_t &= \sum_{x=1}^T x \log x \binom{T}{x} \ell^x \sum_{v=0}^{T-x} (-1)^v \ell^v \binom{T-x}{v} B_{s_1, T}(T-x-v) \\
&= \sum_{x=1}^T \sum_{v=0}^{T-x} x \log x \binom{T}{x} \binom{T-x}{v} \ell^{x+v} (-1)^v B_{s_1, T}(T-x-v) \\
&= \sum_{x=1}^T \sum_{v=0}^{T-x} x \log x \binom{T}{x+v} \binom{x+v}{x} \ell^{x+v} (-1)^v B_{s_1, T}(T-x-v) \\
&= \sum_{i=1}^T \sum_{x=1}^i x \log x \binom{T}{i} \binom{i}{x} \ell^i (-1)^{i-x} B_{s_1, T}(T-i) \\
&= \sum_{i=1}^T \binom{T}{i} \ell^i B_{s_1, T}(T-i) \sum_{x=1}^i (-1)^{i-x} \binom{i}{x} x \log x \\
&= \sum_{i=1}^T \binom{T}{i} \ell^i B_{s_1, T}(T-i) \sum_{x=1}^i (-1)^{i-x} i \binom{i-1}{x-1} \log x \\
&= T \sum_{i=1}^T \binom{T-1}{i-1} \ell^i B_{s_1, T}(T-i) \sum_{x=1}^i (-1)^{i-x} \binom{i-1}{x-1} \log x. \tag{11}
\end{aligned}$$

Also, we can write

$$B_{s_1, T}(T-x) = \underbrace{\sum_{\ell_1=0}^{\ell} \cdots \sum_{\ell_{T-x}=0}^{\ell} \sum_{y=0}^{m-T\ell}}_{\sum_{i=1}^{T-x} \ell_i + y = s_1 - x(\ell-1)} \binom{\ell}{\ell_1} \cdots \binom{\ell}{\ell_{T-x}} \binom{m-T\ell}{y} \stackrel{(d)}{=} \binom{m-x\ell}{s_1-x(\ell-1)} \tag{12}$$

where (d) follows by using Vandermonde's identity. Using (7), (11) and (12) thus proves the theorem.